CLAIMS:

1. A method of embedding a digital watermark in an information signal; the method comprising

- providing (415) a watermark secret (106, 430);
- embedding (107,410) a digital watermark (421) in an information signal (101,414) where said embedding is controlled by the watermark secret;
- calculating (102,404) a digital fingerprint (103) from the information signal;
- storing (104) the calculated digital fingerprint as a reference digital fingerprint and storing, in relation to the reference digital fingerprint, a identifier data item (SID) from which the watermark secret can be derived.

2. A method according to claim 1, wherein the information signal is an audio signal, the digital fingerprint is an audio fingerprints, and the digital watermark is an audio watermark.

3. A method according to claim 1 or 2, wherein storing the calculated digital fingerprint and said identifier data item comprises storing the calculated digital fingerprint and the identifier data item in a fingerprint database (105,407).

4. A method according to any one of claims 1 through 3, wherein the watermark secret is related to the calculated fingerprint by a function which is computationally infeasible to invert.

5. A method according to any one of claims 1 through 4, wherein the watermark secret is determined by a random process.

6. A method according to any one of claims 1 through 5, where the digital watermark comprises a watermark payload (419) and wherein the watermark payload is indicative of the information signal.

7. A method according to claim 6, further comprising encoding (420) said watermark payload based on an encryption key (K_P) derived from an identifier (416) indicative of an information content of the information signal.

8. A method according to any one of claims 1 through 7, wherein the information signal is a video signal.

9. A method of detecting a digital watermark in an information signal (500); the method comprising

- providing (407) a plurality of digital reference fingerprints each calculated from a respective reference information signal, where each digital fingerprint is associated with a corresponding watermark secret;
- calculating (404) a digital fingerprint from an information signal;
- determining (502) a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint;
- detecting (505) whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal.

10. A method according to claim 9, wherein determining a matching digital fingerprint comprises sending a query to a fingerprint database, the query comprising the calculated digital fingerprint; and receiving from the fingerprint database a response including a identifier data item from which the watermark secret associated with the matching digital fingerprint can be derived.

11. A method according to claim 10, wherein sending a query and receiving a response comprise communicating via a communications network.

12. A method according to any one of claims 9 through 11, wherein the information signal comprises an encoded information signal; and calculating the digital fingerprint comprises decoding the encoded information signal, and calculating the fingerprint from the decoded information signal.

13. A method according to any one of claims 10 through 12, wherein determining a matching digital fingerprint comprises performing a search in a fingerprint database based on reliability information about the calculated digital fingerprint.

14. An arrangement for embedding a digital watermark in an information signal; the arrangement comprising

- means (107, 428) for embedding a digital watermark in an information signal where said embedding is controlled by a watermark secret;
- means (102, 404) for calculating a digital fingerprint from the information signal; and
- means (105, 407) for storing the calculated digital fingerprint as a reference digital fingerprint and for storing, in relation to the reference digital fingerprint, a identifier data item from which the watermark secret can be derived.

15. An arrangement for detecting a digital watermark in an information signal; the arrangement comprising

- means (105, 407) for providing a plurality of digital reference fingerprints each calculated from a respective reference information signal, where each digital fingerprint is associated with a corresponding watermark secret;
- means (102, 404) for calculating a digital fingerprint from an information signal;
- means (204, 502) for determining a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint; and
- means (202, 505) for detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal.

16. A database system comprising

- a storage medium (105, 407) having stored thereon a plurality of digital reference fingerprints each calculated from a respective reference information signal, and having stored thereon, in relation to each of the digital reference fingerprints, a respective identifier data item from which a corresponding watermark secret associated to said digital fingerprint can be derived;
- means (301) for receiving a request from a watermark processing system for a watermark secret suitable as an input for embedding a digital watermark in an

information signal, the request comprising a digital fingerprint calculated from the information signal by the watermark processing system;

- means (303) for determining a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint; and
- means (304) for sending a response to the watermark processing system, the response comprising the identifier data item stored in relation to the determined matching digital fingerprint.